Symantec Management Platform 7.1 MP1 Release Notes

Symantec

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Altiris, and any Altiris or Symantec trademarks used in the product are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Symantec Management Platform 7.1 MP1 Release Notes

This document includes the following topics:

- About Symantec Management Platform 7.1 MP1
- What's new in Symantec Management Platform 7.1 MP1
- General installation and upgrade information
- System requirements
- Installing
- Known issues
- Fixed issues
- Other things to know
- Documentation that is installed
- Other information

About Symantec Management Platform 7.1 MP1

Build number 7.1.6797

The Symantec Management Platform is a group of foundation services that IT-related solutions leverage. Solutions integrate with the platform and take

advantage of the shared services, such as security, reporting, communications, package deployment, the Configuration Management Database (CMDB), and more.

What's new in Symantec Management Platform 7.1 MP1

The following table lists the features that are new in Symantec Management Platform 7.1 MP1.

Table 1-1 New features in Symantec Management Platform 7.1 MP1

Feature	Description
Changes to security roles	Symantec Management Platform 7.1 has its own user accounts. Previous versions of Symantec Management Platform used Windows users and groups for user security. Windows users are still used, but they are no longer the only security mechanism. Before Symantec Management Platform 7.1, role management involved creating Windows local groups on the Symantec Management Platform server for roles and then adding Windows users to them. In Symantec Management Platform 7.1 onwards, the Symantec Management Platform maintains its own list of user accounts and roles. These accounts and roles can be imported from Windows. This import occurs if you upgrade to Symantec Management Platform 7.1 so access is not interrupted and security is maintained. User accounts, which are sometimes referred to as users, are not the same as user resources in Symantec Management Platform. A user resource is an entity that is used to associate managed devices with the owner of the device. The existing user resources and the user accounts that can log on to the Symantec Management Console or run a workflow are separate entities. Each Symantec Management Platform user account contains the credentials that the user needs to access the Symantec Management Console or to run a workflow. The credentials may be internal Symantec Management Platform user names and passwords or Windows accounts. Internal credentials are currently used for workflow integration only. Windows credentials are required to access the Symantec Management Console. The Everyone role is a top-level role that contains all roles and user accounts. This role replaces the Windows built-in groups Everyone and Authenticated Users. Security roles can now be nested. You can add a role to multiple security roles. A member of multiple security roles has the union of all the privileges and permissions that those roles grant. When setting up security, see "Setting up Symantec Management Platform security" in the Symantec Management Platform User Guide. This section contains updated information to help guide you through security setup and configuration.

Table 1-1 New features in Symantec Management Platform 7.1 MP1 *(continued)*

Feature	Description
Windows Server 2008 R2 required	You must install Symantec Management Platform 7.1 on a computer running Windows Server 2008 R2. Windows Server 2008 R2 requires a 64-bit computer. If you upgrade to Symantec Management Platform 7.1, Symantec recommends that you upgrade on a new computer. However, if your current computer is a 64-bit computer, you can upgrade on that computer. Before you upgrade, you must back up all of your data and upgrade your operating system. Service packs to Windows Server 2008 R2 are not supported.
Secure server required	You must install Symantec Management Platform 7.1 on a secure server. If you want, you can have Symantec Installation Manager set up your Notification Server as secure server during the installation process.
Delegating Network Discovery tasks to non-administrators	The top-level network administrator can now delegate discovery tasks to other users who are not administrators. Admin-level roles in Symantec Management Platform security are Administrator and Symantec Supervisors. These are default, or predefined, security roles. Now the administrator can delegate discovery tasks to non-administrator roles. Some of the predefined security roles are Symantec Level 1 Worker and Symantec Level 2 Worker. To enable users to discover network devices and work with connection profiles and credentials, you set permissions. You also assign privileges to user roles to enable them to create connection profiles and credentials. You set permissions on the items that you want the users to work with: the connection profiles and credentials. Then, you select a non-administrator user role to which you assign users. You then limit or augment the scope of the role by removing or assigning specific privileges.
Policy for remote installation of Pluggable Protocols Architecture (PPA)	Pluggable Protocols Architecture (PPA) includes a policy that can remotely install the Pluggable Protocols Architecture (PPA) client computer component on a site server. You must install this component on a site server before you can add monitor service to the site server. When the Pluggable Protocols Architecture (PPA) client computer component is installed, the credential manager client computer component is also installed. The policy that installs the credential manager client computer component configures the agent to automatically import credentials from Notification Server.
Concurrent package downloading with UNIX, Linux, and Mac	UNIX, Linux, Mac supports concurrent package downloading with Managed Software Delivery if the policy contains more than one package.

Table 1-1 New features in Symantec Management Platform 7.1 MP1 *(continued)*

Feature	Description
Data migration	When you upgrade from Symantec Management Platform 7.0 to Symantec Management Platform 7.1, you can migrate all of the data in the CMDB. You migrate the data in the database by pointing to the database during installation. You can also migrate Notification Server settings and the general settings that are not in the CMDB with the Symantec Notification Server Migration Wizard. For example, you can migrate KMS keys, credential manager keys, and security roles.
Installation of SQL Server Express	If you do not have SQL Server installed, you can let Symantec Installation Manager install Windows SQL Server Express near the beginning of the installation process. You can use SQL Server Express if you manage less than 500 computers.
Enhanced console views	If you install Symantec Management Platform and accompanying versions of the following products, you see enhanced console views: ■ Deployment Solution standalone ■ IT Management Suite ■ Server Management Suite ■ Client Management Suite **Note:** The enhanced views appear only if you install Deployment Solution as a standalone product or if you install one or more of the full suites that are listed. If you install one or more solutions individually without installing the full suite first, then the enhanced views do not appear. A getting started guide for users who have installed one of the listed products is available at the Symantec documentation Web site. ITMS Enhanced Console Views Getting Started Guide

General installation and upgrade information

You use Symantec Installation Manager to install Symantec Management Platform and all of the products that run on the platform. You also use Symantec Installation Manager to install updates, apply licenses, and repair installations.

Refer to the following guides as needed for detailed information about planning, implementation, and migration:

- IT Management Suite Planning and Implementation Guide
- IT Management Suite Migration Guide v6x to 7.1

- IT Management Suite Migration Guide v7.0 to v7.1

The following third-party plug-ins are prerequisites for Symantec Management Platform 7.1:

- Sun Java Runtime 6
  Java JRE is required for LiveState and Altiris Package Conversion. Java JRE is also required on any computer that remotely accesses the Symantec Management Console when the Software Library is used as the package source.
- Microsoft Silverlight 3.0
  Silverlight is required for the deployment portal of Deployment Solution and the First Time Setup page in the Symantec Management Console.
  The enhanced console views use Silverlight technology and do not support IME input in text boxes. This is a known limitation of Silverlight in windowless mode.
- Adobe Flash Player 10
  The Adobe Flash Player plug-in for Internet Explorer is required for the Resource Association Diagram in the Asset Management Suite.

When you upgrade from Symantec Management Platform 7.0, you can migrate all of the data in the 7.0 Configuration Management Database (CMDB). Because the 7.0 database is compatible with Symantec Management Platform 7.1, you can connect to an instance of the database to migrate the data. Symantec recommends that you connect to the 7.0 database during installation. You can connect to the database on the **Database Configuration** page in Symantec Installation Manager.

However, the following Notification Server data is not stored in the database and must be migrated separately:

- Notification Server security settings and some general settings
  You can migrate these settings with the Altiris Notification Server Migration Wizard.
- Windows Server user accounts
  You must recreate the user accounts on the new computer.
- Some solution-specific files and settings
  You must manually move some solution-specific files and settings.
- Hierarchical relationships
  If you use hierarchical relationships, you must recreate them and enable replication.

For more information about upgrading, see the documents at https://www-secure.symantec.com/connect/articles/altiris-endpoint-management-migrations-and-upgrades-71.

System requirements

The recommended system requirements vary depending on the size of the environment. The size of the environment also affects how you configure the platform.

For more information, see the IT Management Suite Planning and Implementation Guide.

- Symantec Management Platform 7.1.
- Symantec Management Platform 7.1 requires Windows Server 2008 R2 (64-bit). Service packs to Windows Server 2008 R2 are not supported.
- Adobe Flash.
  You must install Adobe Flash for the Topology Viewer control to function correctly. If you are running Notification Server in secure mode (HTTPs), ensure that you have Adobe Flash installed. For details, please see TECH46641

Installing

Refer to the IT Management Suite Planning and Implementation Guide for details.

Known issues

The following are known issues for this release. If additional information about an issue is available, you can click the corresponding article link to read it.

For the most up-to-date information, latest workarounds, and other technical support information for this product, see the Technical Support knowledge base.

The known issues are separated into the following components:

- Symantec Installation Manager
  Table 1-2
- Notification Server
  Table 1-3
- Task Server
  Table 1-4
  See the Technical Support knowledge base.
- Software Management Framework
  Table 1-5
- Data Connector
  Table 1-6

- Network Discovery
  See Table 1-7 on page 22.
- Credential Manager, Connection Profiles, and the Pluggable Protocols Architecture
  Table 1-8
- UNIX/Linux/Mac
  Table 1-9
- Symantec Management Console
  See Table 1-10 on page 28.

Table 1-2 Known Issues for Symantec Installation Manager

Issue	Description	Article Link
The licenses 'In Use' count is not visible on Product Licensing in SIM	This is by design.	N/A
Some licenses do not appear correctly on the **Product Licensing**	If you install IT Management Suite and do not apply licenses, Symantec Installation Manager (SIM) should apply extended trial licenses (30 days). However, if SIM cannot contact the licensing server, it will apply a regular trial license (7 days). The **Product Licensing** page will show these as regular trial licenses rather than the extended trial licenses.	N/A
SQL Server name does not populate on the **Database Configuration** page during installation	When no network is enabled, the SQL Server name does not get populated automatically on the **Database Configuration** page. To resolve this issue, you can do one of the following: ■ Enter the SQL Server name manually. ■ Have SQL Server Browser enabled (Microsoft KB: http://msdn.microsoft.com/en-us/library/ms181087.aspx). ■ Enable Named-Pipe Protocol.	N/A
Sometimes unable to apply additional licenses to some products	If you have pcAnywhere or Deployment Solution installed with 100 licenses applied and you try to apply an additional 1000 licenses, the licenses do not get applied. The error message indicates that you need to apply licenses with a later date over the existing licenses.	TECH133385

Table 1-2 Known Issues for Symantec Installation Manager *(continued)*

Issue	Description	Article Link
Certificate file does not persist on the **Notification Server Configuration** page	If you select a certificate (PFX file) on the **Notification Server Configuration** page and later navigate back to this page, the certificate is no longer listed on the page. The solution is to reimport the certificate.	N/A
Extracting an IT Management Suite package to a non-default location causes a problem with the product listing file	If you extract the IT Management Suite package to a non-default location, the product listing is not extracted to the location where Symantec Installation Manager looks for it. For example, if you extract the package on drive E, the product listing is extracted to E:\Components\symantec.pl.xml. Symantec Installation Manager looks for the product listing file at E:\Altiris\Symantec Installation Manager\Installs\Altiris\symantec.pl.xml. To resolve this issue, change where Symantec Installation Manager looks for the product listing file to the location where it was extracted.	N/A
Uninstall leaves many files and folders	After you uninstall the Symantec Management Platform products many files, registry keys and values, and directories are not uninstalled. You can remove these items with the SmpZap command line utility. The Article ID link accesses a knowledge base article with instructions for using this utility and with the utility's files attached.	TECH42647

Table 1-3 Known Issues for Notification Server

Issue	Description	Article Link
Users in AD **Distribution Groups** are imported and are able to log on to NS server	Users in the **Distribution Groups** should not be able to log on to the Symantec Management Platform server with Symantec Supervisors access rights. To correct this situation, when importing you should filter out the **Distribution Groups** and import only **Security Groups**. When doing the Authentication and Authorization check for a user, if the user is found only in **Distribution Group**, deny access to the NS server. This issue will be fixed in a subsequent release.	N/A

Table 1-3 Known Issues for Notification Server *(continued)*

Issue	Description	Article Link
Unable to assign permissions to a role in a non-English environment	In a non-English environment, you cannot give a role additional permissions other than 'read'. The workaround is to click the **Advanced** option in the Security Role Manager and use it to add permissions.	N/A
Unhandled exception occurs when console tree nodes are loaded during hierarchy replication	If you have a parent-to-child hierarchy and you run the complete replication schedules or the differential replication schedules to replicate from parent to child, you may see an error. When you access **All Settings** on the **Settings** menu of the child, the console may not load but may display the **Symantec Management Server Error** page.	N/A
Computer name does not appear in a report for computers with double-byte characters in their name	If a client computer has double-byte characters in its name, the **Name** column of the Agent Installation Status report is blank.	N/A
Unable to clone a role if the copy uses double-byte or a surrogate string in its name	If you create a role and then clone it and use double-byte characters or a surrogate string in its name, the role fails to get cloned.	N/A
Unable to edit predefined tasks in the Managed Software Delivery Wizard	In the Managed Software Delivery wizard, an unexpected exception is thrown when you try to edit a predefined task. The exception does not occur for tasks that you create.	N/A
Client computer cannot download packages with a long path depth	If a software package has a path depth longer than 256 characters, a client computer cannot download the file.	N/A
Unable to save files that are added for metering purposes	The **Add Software Product** dialog box has a **Meter/track usage** tab. You can click the **Add Program** option on this tab to add a program to meter. However, when you click **OK** to save the product, the files are not saved.	N/A
Restart of Notification Server services is required after reconfiguring the database from the console	When upgrading from DMC 1.1 to DMC 2.0, if you connect to the old database on the Database Settings page in the console, you must restart Notification Server services before you can execute any tasks. Symantec recommends that you connect to your restored 7.0 CMDB from the **Database Configuration** page in Symantec Installation Manager and not from the console.	N/A

Table 1-3 Known Issues for Notification Server *(continued)*

Issue	Description	Article Link
Limit new hierarchies to only two levels	Symantec recommends that you limit new hierarchies to two levels. A Notification Server that is a child should not also be a parent.	N/A
The Symantec Management Agent crashes when package server is installed on a computer where the default Web site inside IIS has been removed	Package server does not support hosting packages within a non-default Web site. The default Web site must exist within IIS for the package server to function normally. When no default Web site exists within IIS, the Symantec Management Agent crashes even if the 'Publish HTTP(s) codebases' option is disabled and only the 'Publish UNC codebases' option is enabled within the package service settings. This issue will be resolved in a future release.	N/A
Creating new AP creates error and a warning-level message is logged	When you create a new automation policy, an error is generated and warning messages are logged. However, after you create the policy you can load it, change settings, and save it without the error recurring.	N/A
The Create Resource Targets privilege is not currently used	Any user who has the permission Apply to Resource Targets can create resource targets. Enabling or disabling the Create Resource Targets privilege (menu path: Settings > Security > Roles, then select the Privileges tab) has no effect. If you want to prevent a user from creating resource targets you need to remove the Apply to Resource Targets permission from that user. Removing this permission means that the user cannot open the resource selector dialog box.	N/A
Attempts to access the Symantec Management Console using the FQDN in the console URL may fail with an error message	If the Symantec Management Console is set up to use a non-default port, when you try to add computers on the **Agent Push** page of the console by FQDN (non-localhost), an exception error occurs. The following error message is displayed: Data for the page you are currently viewing has expired. To resolve this issue, use the appropriate IP address in the console URL instead of FQDN.	TECH121988

Table 1-3 Known Issues for Notification Server *(continued)*

Issue	Description	Article Link
Replicated Symantec Management Agent Settings - Targeted policy can be edited or deleted on child Notification Servers	If you replicate the Targeted Agent Settings policy (in the Settings tree: **Settings > Agents/Plug-ins > Symantec Management Agent > Settings > Symantec Management Agent Settings - Targeted**) to child Notification Servers, the replicated policy is editable on the children. This is not correct behavior. Replicated system policies should be read-only on child Notification Servers, and you should not be able to modify or delete them. Note that any changes that you make to this policy on a child Notification Server is overwritten on the next replication schedule, when the same policy is replicated again from the parent.	N/A
Non-Latin characters are not displayed correctly when used in custom data class attribute names	When you create a custom data class (in Inventory Solution, in the **Inventory Solution Settings** folder, on the **Manage Custom Dataclass** page) and specify the attribute names that contain non-Latin characters, the characters are initially displayed correctly in the console page. However, when you click **Save Changes** to save the new data class, the names are replaced with question marks (??). This issue affects only the languages that use non-Latin characters. Inventory Solution must be installed to access the custom data class functionality.	N/A
Drill-down reports fail when the drill-down targets a remote Notification Server that uses a non-default port	If you have a hierarchy of Notification Servers, some reports display summary data for each Notification Server. These reports let you drill down into the results by clicking the appropriate row in the results grid for detailed data about a particular Notification Server. However, if a Notification Server is installed to a non-default Web site and port, its summary data is displayed correctly in the summary report but any attempt to drill down to display the detailed data fails. A new browser window opens to display the report results, but it contains a Server Error message telling you that the resource cannot be found.	TECH46377

Table 1-3 Known Issues for Notification Server *(continued)*

Issue	Description	Article Link
Report filter conditions are sometimes lost when you edit the report in the Query Builder	When you create a report using the Query Builder, you can specify filter conditions in the **Filter Expressions** tab. However, when you later edit the report, some filter conditions may be dropped from the report query. This happens whether or not you opened the **Filter Expressions** tab: when you save the modified report, some conditions may no longer appear in the report query.	TECH42219

Table 1-4 Known Issues for Task Server

Issue	Description	Article Link
Error in agent logs	The following error message sometimes appears in agent logs: "Failed to create object TaskServerHandler: The operation completed successfully".	N/A
Server tasks do not work when you reconfigure the database from the Database Settings page	When you upgrade and point to the old database on the **Database Settings** page, you cannot run any server tasks until you manually restart the Altiris, ATRSHOST, and CTDataload services. If you point to the old database on the **Database Configuration** page in Symantec Installation Manager during installation, you do not encounter this issue.	N/A
Task server unable to run tasks using 7.0 task servers after you upgrade to Symantec Management Platform 7.1	After you upgrade to Symantec Management Platform 7.1, you must upgrade your 7.0 task servers before you can use them to run tasks.	N/A
Unable to run the tasks that were created in 7.0 task servers after network server is upgraded to 7.1	Tasks that were created in the 7.0 task servers are not supported in the 7.1 environment.	N/A
Initial use of '.\username' causes any script tasks specified as Machinename\username) to fail with error 'Unable to open the file' because of Profile loading problem	This issue applies only to some operating systems, such as Window XP SP2 and Windows 2003. It does not apply to pre-Vista versions such as Windows 7 or Windows Vista Ultimate SP2.	N/A

Table 1-4 Known Issues for Task Server *(continued)*

Issue	Description	Article Link
Task Server Task runs even though "Allow other tasks to run while running this task" is checked	If you create a task and uncheck the option **Allow other tasks to run whil running this task**, other tasks can still run.	N/A
Changing the tickle port in config and UI does not cause the tickle port to actually change	If you change the tickle port under **Site Server** settings, or in the config from the default of 50123, the change is not made. The server will continue trying to open 50123 which causes 'unable to connect to tickle server' errors in the log.	
Task Server needs to be restarted after a new database has been created	When you create a new database, you need to restart task server (Altiris Object Host Service) from the Windows service console. This is required to make the previously scheduled PM import task run.	TECH45090
Tasks that are contained within jobs must be migrated separately	When you migrate a job from 6.0 to 7.1, you also need to migrate the associated tasks. The tasks that are included in the job are not migrated automatically with the job.	N/A

Table 1-5 Known Issues for Software Management Framework

Issue	Description	Article Link
Quick Delivery tasks fail to execute by timeout when maintenance window is set up on clients	If you create a Quick Delivery task and the task times out before the maintenance window is activated on the client, the task fails. By default, a task times out after 30 minutes. You can change when a task ends on the **Task options** tab of the Advanced settings.	N/A
Software component with version and company resources do not get associated until the following day after a Software Discovery	The associations should be made as data is processed, but the associations are made when the Notification Server daily schedule runs.	TECH150132
The auto generated TAR extraction command line does not work on some UNIX computers	The command line generator creates the following command line for TAR archives: "tar xvfz <package>". This command will not run on some UNIX and Linux computers that do not support the "z" option. For these computers, create the command line manually.	N/A

Table 1-5 Known Issues for Software Management Framework *(continued)*

Issue	Description	Article Link
A Managed Software Delivery policy that was scheduled to run once runs whenever the user logs on	A Managed Software Delivery policy that targeted a user and was scheduled to run only once runs each time the targeted user logs on.	N/A
Applicability check issues with a Managed Software Delivery policy	If a Managed Software Delivery delivers two software resources and the second software resource is dependent on the first software resource, the applicability check for the second resource fails because this check runs before the first software resource is installed.	N/A
Applications with large installation paths fail to execute	With a Managed Software Delivery policy or Quick Delivery task, applications with large installation paths fail to execute.	TECH133459
Software Catalog and Software Library settings do not replicate with “Replicate now” or “Replicate to” methods	Changes made to any of the settings found in the Software Catalog and Software Library Settings folder are not replicated when a “Replicate now” or “Replicate to” method of replication is invoked.	N/A

Table 1-6 Known Issues for Data Connector

Issue	Description	Article Link
Unhandled exception occurs when testing an incomplete OLEDB data source	If you are configuring an OLEDB data source and the configuration is incomplete and you use the “Test data source” feature before saving the page, the page crashes and displays an unhandled exception message. If you save the page before using “Test data source,” the page properly reports the incomplete configuration without crashing. If the page crashes, changes made in the page might be lost. However, you can re-enter the configuration information by reloading the page.	N/A
Script errors with connector rules opened from "Connector rules health check Task"	After running "Connector rules Health Check Task," if you select “Task Instance Details” to view the details of running the task and then click on a rule to open the rule configuration page, you get the error "top.windowManager is null or not an object" and you will not be able to modify the rule.	N/A

Table 1-6 Known Issues for Data Connector *(continued)*

Issue	Description	Article Link
Collection migration issue	Data connector v6.x can have CMDB Rules, Resource Export Rules, and Bulk Resource Export Rules which use “Collections.” During the migration process, the “Collections” used by those rules are converted to “Resource Targets,” and “Resource Targets” that are converted from the “Collections” should contain the same memberships as the legacy “Collections.” In this release, the converting process is not functioning properly; the “Resource targets” converted from the legacy “Collections” do not contain memberships. To work around, you need to re-create the “Resource Targets” for those rules by using the legacy “Collections” to make them work properly.	N/A

Table 1-7 Known Issues for Network Discovery

Issue	Description	Article Link
Exception in NS log during upgrade with hierarchy	When running the hierarchy differential replication schedule in certain upgrade scenarios, you may get exceptions such as "Incompatible columns in DataClassAttribute. Error:Class Name: VM Guest" in the NS log. Break the hierarchy prior to upgrading. Then, upgrade both parent and children before re-joining.	TECH154203

Table 1-8 Known Issues for Credential Manager, Connection Profiles, and the Pluggable Protocols Architecture

Issue	Description	Article Link
Server error occurs while adding categories	While adding categories to Alert Management Settings, you see a server error. This issue will be fixed in a subsequent release.	TECH154205

Table 1-8 Known Issues for Credential Manager, Connection Profiles, and the Pluggable Protocols Architecture *(continued)*

Issue	Description	Article Link
All remote RMSes crash after DMC 2.0 installation over ITMS 7.1 MR1	If you are running ITMS 7.1 using a remote RMS server, and then you install DMC 2.0, the remote RMS server crashes. Right after you install ITMS 7.1 MP1, before you install DMC 2.0, manually disable the PPA agentconfiguration policy. Warning! Do not confuse the agentconfiguration policy with the agent _rollout_ policies. Do not disable the agent_rollout_policies.	N/A
Altiris object host service is crashing while running the VMM inventory task on multiple hypervisors	To work around this issue, run the VMM inventory task one hypervisor at a time.	N/A
WS-MAN protocol is disabled and all settings are set to default after upgrade to PPA SP4 7.0.7416	To work around this issue, manually enable WS-MAN protocol, specify custom credentials from the drop-down menu, and reset all settings.	N/A
When creating or editing Credentials or a Profile, the password fields are left blank (no asterisks appear)	The asterisks appear as the password is entered, but after that, when the password field is displayed, the field is empty. This happens when the password field is displayed in the profile manager or the credential manager.	N/A
PPA CacheManager is deleting its internal state before it gets fresh data from NS, which causes empty cache data when NS server restarts	The original issue was fixed. However, now Monitor Metrics may time out while PPA retrieves data. To ensure that cache data is accurate, configure your metrics, including setting proper polling intervals, to account for possible server downtime.	TECH153674
2008R2 x64 - Impossible to perform monitoring, using WMI, HTTP, SNMP protocols, because it fails to resolve credentials from Credential Manager with Inner exception	You must enable WCF Activation to allow for using protocols other than HTTPS.	TECH140507

Table 1-8 Known Issues for Credential Manager, Connection Profiles, and the Pluggable Protocols Architecture *(continued)*

Issue	Description	Article Link
WMI, WSMAN, and other monitoring plug-ins become unavailable if multiple web-service identities are used	You must ensure that you remove multiple identities if you choose a custom Web site.	TECH142631

Table 1-9 Known Issues for UNIX/Linux/Mac

Issue	Description	Article Link
ULM Agent 7.0.4541: incorrect time is returned by the agent after manual change of timezone on client systems	After you make a timezone change on a UNIX/Linux/Mac client, the change may not affect running services until after you restart the client system.	TECH153660 N/A
Managed delivery with Linux rpm upgrade does not work	Currently the ULM agent does not support upgrade of RPMs. As a workaround uninstall the old rpm using Managed Delivery first and then perform a new rollout.	N/A
Active user change notification does not work in ULM	Currently the ULM agent does not support user-based policies, so a policy is not executed on user login. Schedule type "At user login" is supported but for the Mac platform only.	N/A
Altiris: Linux agent push status reports success after the client installation fails	As ULM supports only event-based status reporting, the last successful status is sometimes shown while the rollout has failed. The "Remote install finished: Success" status indicates a fully successful installation.	N/A
Clients with unsupported OSes are listed as PS candidates	If an Apache server is configured on a Linux desktop computer with the ULM agent installed, it may appear as a suitable candidate for package server . However, because Apache is not bundled with Linux desktops (RedHat, SUSE), Symantec does not officially support running PS on Linux desktop computers.	N/A

Table 1-9 Known Issues for UNIX/Linux/Mac *(continued)*

Issue	Description	Article Link
Keys generation for depot files is broken. Only the package name is available that is used as a key during the import process (without any OS name or architecture)	Some ULM software packages not containing architecture and supported OS version information may be detected during import as the same package. As a workaround, rename one of the conflicting packages.	N/A
Managed delivery policy does not detect already installed software when it is delivered in archived format	After software is delivered in archived format, the ULM agent cannot track the installed software but can only track the archived package. Software is only marked as uninstalled after you generate the uninstall type command for the same software package and schedule it to the client. To execute the uninstall policy successfully (exit code 0), the software must be removed from SMF. Edit the command manually to uninstall the software.	N/A
HttpdIntegration does not properly parse Apache config file with SSL and custom	Known limitations exist on supported Apache configurations for the computer that is intended as a package server candidate. Please avoid using complex Apache configurations on such computers.	N/A
HttpdIntegration does not use apache_config_location parameter in client.conf	Known limitations exist on supported Apache configurations for the computer that is intended as a package server candidate. Please avoid using complex Apache configurations on such computers.	N/A
You can enable a package server password when "Publish HTTP codebase" is enabled	A certain security risk exists if you disable anonymous access to a Linux package server in HTTP mode. Linux package servers support only "basic authentication." This means that passwords are sent in plain text. Please either use HTTPS or keep anonymous HTTP access for a Linux package server.	N/A
Impossible to reset proxy settings by "AeX-configure -iconfigure"	You cannot reset enabled proxy settings from the client. Disable proxy by updating the corresponding configuration policy in SMP Symantec Management Console.	N/A

Table 1-9 Known Issues for UNIX/Linux/Mac *(continued)*

Issue	Description	Article Link
Software Management Framework agent does not send a full software inventory if the Notification Server computer was changed	If the ULM agent was manually redirected to another Notification Server, a full software inventory is not sent. The workaround is to stop the agent, delete the swc.dat file, and restart the agent.	N/A
Sometimes Push install fails	A Push installation of the ULM agent can fail with the message "The 'cd' command failed." As a workaround, repeat the Push install.	N/A
Timezone, OS language, Primary User, and host id are missing under Resource Summary	Some basic inventory information may not be reported for certain ULM systems (Solaris, HP-UX, and RedHat).	N/A
The **Allow user to interact with installing software** option does not function on Mac OS	When you set this option as part of a Managed Software Delivery for Mac, the option does not work. The notification pop-up may appear (if you are logged into the shell), but it is non-functional.	N/A
If you attempt to disable proxy usage by running "AeX-configure" from the client, proxy settings are not reset and you may lose connectivity for the client	To avoid this issue, you should disable or change proxy settings from the Symantec Management Console only. If you lose connectivity because of this issue, reinstall the Symantec Management Agent by performing a PUSH installation from the Symantec Management Console. When you reinstall, uncheck the "Keep the current Symantec Management Agent settings if possible" option to specify not to save the current configuration. The agent is successfully reinstalled without using proxy settings, and connectivity is restored.	N/A

Table 1-9 Known Issues for UNIX/Linux/Mac *(continued)*

Issue	Description	Article Link
If you select a service action for AIX inittab services in a UNIX/Linux/Mac Service Control task, the task fails with an error message	The AIX inittab service does not support any of the actions that are available in the **Service Action** drop-down list. When the AIX inittab service is checked, the Service Action field should be grayed out and not selectable. At present this field is (incorrectly) functional in the Symantec Management Console. To avoid errors in your Service Control task, you need to set the Service Action field to No action. This action prevents any attempt to execute Start, Stop, Restart, or Get Status commands for AIX inittab services. Note that currently the No action setting is incorrectly processed and cannot be used for task creation. As a result, all Service Control tasks that are created for the inittab service control system are reported as failed, with the error message "Missing or invalid service action" displayed. This message appears regardless of whether the specified process or service was successfully modified.	TECH46454
RTE Command Line Builder generates an incorrect install command	When you manually create a software package that contains .rte files and use RTE Command Line Builder to generate the appropriate installation command line, the package installation may fail. The command line is the command to execute the installation file on client systems. This failure can occur because the generated command line contains the %SIFNAME% token. This token is added as a part of the command and is not replaced on the client system with the software installation file name. This issue results in a failing installation of the software on client systems. For manually created packages containing .rte files,replace the %SIFNAME% token with the appropriate file name.	TECH46206
You cannot use an upgrade policy to upgrade the Symantec Management Agent for UNIX and Linux to version 7.1 from version 6.2.1378 on HP-UX computers with IPv6 enabled	The simplest way to work around this issue is to upgrade to Symantec Management Agent 7.1 using the Push installation method. Alternatively, you can disable IPv6 on the target computer.	TECH42029

Table 1-10 Known Issues for Symantec Management Console enhanced console views

Issue	Description	Article Link
Silverlight does not support IME input	The enhanced console views use Silverlight technology and do not support IME input in text boxes. This is a known limitation of Silverlight in windowless mode.	N/A
Software metering is not enabled automatically	This issue occurs when you are working in Symantec Management Console > Manage > Software. To meter software, you must manually identify the software program that you want to track. In certain cases you see a warning that instructs you to enable metering. Note that you can only meter software if you have Inventory Solution (CMS, SMS, or ITMS) installed.	N/A
Drag and drop does not work with organizational groups and organizational views	This issue occurs when you are working in Symantec Management Console > Manage > Computers. Currently, you cannot drag and drop organizational groups onto organizational views.	N/A

Fixed issues

The fixed issues are separated into the following components:

- Symantec Installation Manager
  Table 1-11
- Notification Server
  Table 1-12
- Task Server
  Table 1-13
- Software Management Framework
  Table 1-14
- Data Connector
  Table 1-15
- Network Discovery
  Table 1-16

- Credential Manager, Connection Profiles, and the Pluggable Protocols Architecture
  Table 1-17
- UNIX/Linux/Mac
  See Table 1-18 on page 43.

Table 1-11 Fixed Issues for Symantec Installation Manager

Issue	Description	Article Link
Unable to add optional components to an installation package if components were already installed on server	If you installed optional components(docs, languages, and migration) to a server and then attempted to create an installation package on that server, you could not add those components.	N/A
Unable to uninstall a product without updating Symantec Installation Manager to the latest version	If you do not have the latest version of Symantec Installation Manager installed, you could not uninstall any product without first installing the latest version of Symantec Installation Manager.	N/A
Symantec Installation Manager ran a full configure on an existing database	Symantec Installation Manager ran a full config when it was pointed to an existing database.	N/A
A non-default Web site with the default SSL port caused errors	On the Notification Server Configuration page, if you selected a non-default Web site and bond it to the default SSL port, an error appeared.	N/A
Console did not launch when Symantec Management Platform was installed using proxy settings which are bypassed	If you checked the IE proxy setting **By pass proxy settings** and then checked **Use SSL to access the Management Platform** on the Notification Server Configuration page, you encountered problems accessing the console.	N/A
SQL server information is now updated in the Help	SQL server information was not updated in the Help.	N/A
Offline installations were not supported.	Any suite could not be installed on 64 bit OS if at least one product has 32-bit package . This issue is fixed.	N/A

Table 1-11 Fixed Issues for Symantec Installation Manager *(continued)*

Issue	Description	Article Link
Add recommendation to install SQL Server 2008 in the dialog box	When you run installation of Symantec Management Platform, and choose SQL Express DB Server, a dialog box appears with the message, You should install on SQL Server 2005. Now the dialog box text is changed to You should install Notification Server on Microsoft SQL Server 2005 or Microsoft SQL Server 2008 for best performance.	N/A
Need to export KMS data before installing 7.1	SIM now lets you install the migration wizard and build migration packages before Notification Server is installed. To create migration packages and install the migration wizard before Notification Server is installed, do the following: ■ Install SIM version 7.1 or greater on the new computer. ■ Run SIM ■ Choose Install option components on the Installed Products view. ■ Check the Install Migration Wizard components for migrating Notification Server six data. ■ Follow the rest of the prompts. This process provides you a migration package that you can take to the old computer and get the KMS data to put on the new computer before installing the Notification Server. If Notification Server is already installed or if the PL does not contain the correct migration product, SIM may indicate to you that nothing is available to install after step 3.	N/A
The check box Use SSL to access the Management Platform is not enabled in the SSL settings of IIS Web Site	The check box Use SSL to access the Management Platform was not enabled in the SSL settings of IIS Web Site. The issue is fixed.	N/A
Install Readiness check panel shows Windows 2003 as the recommended operating system	Install Readiness check panel now shows Windows 2008 R2 as the recommended operating system.	N/A
The hyperlink for Microsoft IIS in Install Readiness check panel opens an irrelevant page	The hyperlink for Microsoft IIS in Install Readiness check panel opens an irrelevant page. This issue is fixed.	N/A

Table 1-11 Fixed Issues for Symantec Installation Manager *(continued)*

Issue	Description	Article Link
Unable to install SIM with SMP on OS with localized Administrators localgroup	SIM Installation failed due to SID errors. This issue is fixed.	N/A

Table 1-12 Fixed Issues for Notification Server

Issue	Description	Article Link
Filters did not display the same information for virtual computers as it did for computers	For filters that only contained Virtual Machines, the grid only displayed the **Computer Name** column	TECH142534
Replication did not remove resource associations from the destination Notification Server when they were removed at the source	When resource associations were replicated, only Add and Update changes were made at the destination. Only new items and changes to existing items on the source Notification Server were replicated to the destination. If a resource association was deleted from the source, it is not removed from the destination.	TECH41960
Saving a report as a spreadsheet now functions properly when column values include commas	This issue has been fixed with proper CSV escaping of the column names and the column values when the CSV file is generated. Previously the Save As Spreadsheet option did not save correctly when any data values included commas. The resulting spreadsheet contained jumbled column data.	N/A
When you perform an on-box upgrade from SMP 6.x, the Add Licenses link is missing	This is by design. The Add Licenses link was removed for security reasons.	N/A
Reports that contain non-English characters now display correctly when they are saved in spreadsheet, HTML, or XML format	Previously, when you saved a report that contained non-English characters as a spreadsheet, HTML, or XML file, the non-English characters did not display correctly. This issue has been resolved by correcting the UTF8 encoding so that CSV files are loaded properly.	N/A
You can now specify a raw SQL query as the data source in an automation policy	Previously if you attempted to specify a raw SQL query as the data source for an automation policy, the query was not saved correctly. This issue also affected some SQL queries in filters and reports: in some cases the changes that you made when editing a query were not saved.	N/A

Table 1-12 Fixed Issues for Notification Server *(continued)*

Issue	Description	Article Link
The list of Symantec Management Agent Policies in the Targeted Agent Settings page now displays correctly	Previously the list was restricted to only 10 items and the scroll bars appeared when more items were available. The list did not resize correctly and part of the page was left empty.	N/A
The Notification Server Web is now installed as a subdirectory of the Notification Server installation folder	Previously the Notification Server Web root was the Notification Server installation directory, which was a potential security issue.	N/A
NICs without DNS in a multi-NIC environment are now correctly reported as not having DNS entries	Previously, if you had a multi-NIC environment and some NICs did not have DNS entries, Basic Inventory would incorrectly identify them as having DNS.	N/A
The path names for UNC codebase in package servers are now fully qualified	Previously only the computer name was stored in the package server as part of the codebase cache, so you were unable to use the FQDN. This issue did not affect HTTP codebase: the FQDN was fully recorded in package servers.	N/A
Users that belong to multiple security roles can now access reports reliably	Previously, in some cases where a user belonged to many security roles and only one of those roles had access to a report, the user may have been unable to access the report. Multiple security role IDs were passed to the report: if the list of IDs exceeded a particular threshold, some IDs were lost. Linked to Known Issue KB #49971.	N/A
Packages are now downloaded to package servers if the timestamp does not match the current snapshot	Previously, packages that had file dates newer than those in the snapshot were not downloaded. This scenario sometime occurred when files inside a package on a package server were modified by an out of scope operation such as a virus scanner updating them. Those files were given a file date that was greater than what was expected in the snapshot for that package.	N/A
The Symantec Management Agent now correctly shows the Agent version	Previously, on some operating systems, the Agent version was not reliably reported to Basic Inventory, so did not appear in the Resource Summary page in the Resource Manager.	N/A
NSE priority is now recognized and handled correctly	Previously, the NSE priority was ignored when an NSE was delivered to Notification Server, causing an unacceptable delay in the delivery of critical alerts.	N/A

Table 1-12 Fixed Issues for Notification Server *(continued)*

Issue	Description	Article Link
A warning is displayed when you attempt to assign any site service to an IIS7 computer	Site services such as package server and task server require certain conditions to be met to work correctly on IIS7. The following conditions must be met: ■ IIS6 compatibility modules are installed (to allow creating virtual directories) ■ The default Web site works in the "Classic .NET Application Pool" mode The warning message alerts you to the additional configuration requirements and gives you the option to proceed or cancel the site service rollout process.	N/A
The Search feature now operates correctly on custom SQL reports	Previously, if you attempted to search on a custom SQL report and did not specify any search text, the Edit report page appeared. Only the user-created reports were affected. The predefined reports were not affected.	N/A
Resources are now merged correctly when duplicate GUIDs are created in Hierarchy replication	Previously, in some cases the GUID synchronization at the child Notification Server failed and the resource flip-flopped between two GUIDs. When the resource flip-flopped, both GUIDs were blacklisted, including the currently active one. The result was that the affected agent cannot communicate with the Notification Server. Attempt was made to create a new resource for the blacklisted item but was given the same GUID again.	N/A
In the NS Configurator, the default values in the description fields are now correct	Previously, the default values displayed in the description fields for the following items did not match the actual default values: ■ MaxConCurrentConfigRequests ■ ReplicationProcessorActivityInterval ■ ReplicationMaxJobThreadCount ■ ReplicationMaxEventRows	N/A
The reporting grid now supports the column names that are integers	Previously, when you created a report based on a raw SQL query and named one of the columns as a number, none of the data in that column was displayed.	N/A
Partitioned resources can now be deleted only by users who have appropriate security roles	Previously partitioned resources can be deleted by any user. There was no check on the user's security permissions. This presented both an administration threat, as resources can be lost from the console, and a security threat, as an unregistered user can attack all partitioned resources.	N/A

Table 1-12 Fixed Issues for Notification Server *(continued)*

Issue	Description	Article Link
Hierarchy Rules now have read-only sections where appropriate	For Replication rules with System attributes set, specific controls instead of whole sections are disabled. This also allows links to the resources and data classes to be clickable but prevents modifications. For Relocation rules, the Verification section is hidden. Previously all sections of hierarchy rules were editable, even for the predefined rules that had System attributes set.	N/A
New languages that were introduced in IE8 are now correctly displayed in the Symantec Management Console	Previously the new languages that were introduced in IE8 were not supported and were not defaulting back to standard EN-US. No text strings were displayed in the console. Only the icons were visible. This issue affected the following languages: ■ English (India) [en-IN] ■ English (Malaysia) [en-MY] ■ English (Singapore) [en-SG]	N/A
The Symantec Management Agent now reliably downloads any new files that have been added to a package before running it	Previously, any files that were added to a package were not downloaded to an agent if the agent had already downloaded the package previously. Once a package had been downloaded to an agent, the agent was not getting any updates to that package properly when the package was run at subsequent times.	N/A
Performance enhancement: Notification Server no longer sends multiple Kerberos ticket requests to the Domain Controller	Previously, when you performed a Managed Software Delivery rollout, the Domain Controller received a large number of Kerberos TGT (ticket granting ticket) requests. This sometimes caused the DC to stop responding to other clients on the network that were trying to map network drives, which also requires a TGT from the KDC.	N/A
Item state sizes are now configurable and can be limited to a reasonable size	The Item state size is now controlled by the CoreSettings.config setting ItemStateMaxSizeInKB. The default is 65536 (64MB). You cannot create or save an item that exceeds the maximum size. Previously the item framework allowed the Item State size to grow in an unconstrained manner. These large items could get too large to be loaded and could cause other issues.	N/A
The Resource Explorer Summary Pages now operate correctly	Previously, in some scenarios the Summary page failed to open for a newly discovered resource.	N/A

Table 1-12 Fixed Issues for Notification Server *(continued)*

Issue	Description	Article Link
The Item to delete schedule has had its shared schedule changed from Daily to Quarter Hourly	If you use multiple replication schedules, your SQL disk size will grow rapidly. The replication schedules are generally spaced out during the day so it does not make sense to perform the clean up only at one point during the day. Performing this clean up more often can save SQL disk space. It also means less work in regular chunks, rather than one large delete during the Daily schedule.	N/A
Hierarchy performance has been improved	Previously Hierarchy replication did not scale to more than about 200,000 resources. Large amounts of SQL disk space was used and in some cases replication job items were created that could not be loaded, causing OutOfMemory exceptions. Those exceptions had the knock-on effect of leaving behind the data containers and manifests which never get cleaned up.	N/A
The Licensing Refresh schedule has been modified to improve performance	Previously the Licensing Refresh schedule checked security permissions for every action that is taken. When this was first implemented this was not an issue because these security checks would take place against a cache on the Notification Server. However with Windows 2003 Active Directory the local security cache is only checked as a backup. This means that the AD is being flooded with security checks every time that a new security context is requested. In the case of the Licensing Refresh policy this is happening more then a 1000 times a minute. This is causing issues by overloading the AD.	N/A
Messages that contain % signs are now logged correctly	Previously, the Symantec Management Agent sometimes crashed when it attempted to log a message that included a % sign. This issue was caused by the % sign not being escaped correctly.	N/A
The Agent Push page now operates reliably	Previously the Agent Push status grid failed to load correctly when two push events were present for the same computer with the same _eventTime. This issue effectively disabled the entire push functionality.	N/A
Multiple Active Directory security and distribution groups with the same name are now supported	Windows 2003 domains allow multiple groups (security and distribution type) to have the same name within different parts of the AD tree. Previously, if these "duplicate" groups were present, AD connector would fail to import them.	TECH140499

Table 1-12 Fixed Issues for Notification Server *(continued)*

Issue	Description	Article Link
Package changes in a hierarchy environment are now reflected at child package servers in a reasonable time	Previously changes to replicated packages could take 24 hours to trickle down. During this time the package was not available to site servers and therefore did not make it to endpoints. When package folder content has been modified, once the parent has replicated the package, the child's Notification Server's package server will reflect the changes the next time the agent updates its configuration.	N/A
Symantec Management Platform installs correctly on international operating systems (Spanish, French, German, etc.)	Previously you were unable to install Symantec Management Platform on non-English operating systems. This was due to a localization issue in the MSI file.	N/A
LDAP queries are now filtered to explicitly request the groups that the import rule is configured for	The previous method of importing groups was very inefficient, as the LDAP query simply requested objects of a specific type and then filtered the results. If Active Directory contained a large number of groups, some queries caused Out of Memory exceptions. The LDAP query method has been modified to explicitly request the groups that the import rule is configured for. This results in speed improvements, lower CPU and memory requirements and improved scalability.	N/A
The Delta Update schedule now detects circular references in filters and cancels the update if necessary	Previously only the Complete Update schedule checked for circular references in filters. Circular references in filters were not detected or handled by the Delta Update schedule. This sometimes caused delta updates to consume memory until the service failed.	N/A
The Symantec Management Agent Push Install page now lets you load computers reliably	Previously, in some cases when you attempted to add computers to the grid, a message "Data Could Not Be Loaded" appeared.	N/A
"Unspecified Dataloader Exception encountered for event data class AeX SWD Package" error message is logged to NS log during plug-ins rollout	If this error occurs, incorrect or incomplete information about agents or packages may be stored. This is a known issue for this release. N/A	N/A

Table 1-12 Fixed Issues for Notification Server *(continued)*

Issue	Description	Article Link
The Symantec Management Console did not provide a way to purge old Audit Inventory information from the database	The Inv_Audit table continued to grow as resources were added. To remove old and unwanted data from this table, you had to follow the manual process described in the linked knowledgebase article.	TECH41981
The Purging Maintenance page did not let you purge data from Notification Server 7.0 reports	The Purging Maintenance page only allowed the purging of legacy Notification Server 6.x saved reports. It did not provide the ability to purge Notification Server 7.0 data snapshots.	TECH41488
When the ULM Agent was upgraded from Unix Agent 6.2 to ULM Agent 7.0 SP4 on AIX systems, the $PATH variable had no defined value (paths) in the agent's environment	If no absolute path was allocated, the execution of commands under the agent's environment would fail.	N/A

Table 1-13 Fixed Issues for Task Server

Issue	Description	Article Link
ATRSHOST service was not always created during Task Service upgrade	Sometimes, after you enabled the appropriate Task Server Upgrade policy, the policy ran and the client Task Server appeared to be upgraded. However, the ATRSHOST was not registered and installed as a service and the Task Server did not function.	N/A
Upgraded remote Task Server on 64-bit computer did not work until virtual directory was redirected	The virtual directory of an upgraded remote Task Server referenced C:\Program Files(x86) after Symantec Management Agent was successfully upgraded to 64 bit.	N/A
Command Scripts that contained Cyrillic characters now work	The CTA library code caused this issue. Now, the true agent SDK call is used to write the script file as it honors all platforms correctly.	N/A
CTA logging messages with % signs now do not cause the agent to crash	A script that had %, caused an access violation in the agent and an error message was displayed. The problem was caused by CTA.	N/A
Now you can schedule script tasks that include reserved characters	Previously, a script task that included reserved characters would not execute on the client machine and an error message was displayed. The issue is fixed.	N/A

Table 1-13 Fixed Issues for Task Server *(continued)*

Issue	Description	Article Link
Now Advanced options for all tasks can not be edited on the child Notification Server after complete replication	If you create a hierarchy between two Notification Servers, then after complete replication, the advanced options for all tasks were editable.	N/A
Job or Task Status Detail report now return results	This was a generic problem. The issue is fixed.	N/A

Table 1-14 Fixed Issues for Software Management Framework

Issue	Description	Article Link
A Legacy Software Delivery failed when run for a specified user	With a Legacy Software Delivery , if you selected **Logged on user** in the **Run with rights** drop-down list on the **Advance** tab, the policy failed on the client computer.	N/A
A Managed Software Delivery policy was not activated when user logs on	A Managed Software Delivery policy was not activated on a client computer when the target was user-based and the policy was scheduled to run At user logon.	N/A
Scroll bar in the Software Finder Web part did not work	The scroll bar in the Software Finder Web part did not work.	NA
When a Symantec Software Librarian user first logged into the Symantec Management Console they could not access the My Portal page	The necessary security rights were not given to the Symantec Software Librarian user to view the My Portal page. Now, the user can access the My Portal page.	NA
Some software types were not created for the Software Catalog Data Provider	When the Software Catalog Data provider was configured, some of the new software types were not created.	NA
A Managed Software Delivery policy that was scheduled to run when a computer starts up could fail	With a Managed Software Delivery policy, if you selected the scheduling option, At computer startup, the policy would fail to run when the computer restarted.	NA
A user initiated Managed Software Delivery policy could consume large amounts of CPU	When a user initiated Managed Software Delivery policy ran, the policy would go into an endless loop if the start date for the policy was in the past and if the policy was stuck within a reboot defer. When the policy went into an endless loop, it consumed large amounts of CPU.	NA

Table 1-14 Fixed Issues for Software Management Framework *(continued)*

Issue	Description	Article Link
With a Managed Software Delivery policy, you could not download a package without specifying a command line for the package	If a Managed Software Delivery policy downloaded a package that did not have a specified command line, the package did not download successfully.	NA
Detection rules of Managed Software Delivery Policies that had the same schedule run at the same time	If two Managed Software Delivery policies were scheduled to run at the same time and both policies had detection rules, the detection rules for both policies ran at the same time. This caused issues if the detection rule of one policy was checking to see if the software of the other policy was installed.	N/A
Add button for transforms was disabled in MSI Command Line Builder window	When adding a command line in MSI Command Line Builder for a package that was added using "Access package from a directory on the Notification Server," the Add button for adding a transform was disabled	N/A
A legacy software delivery failed if you selected the “Run with rights” option	When the "Run with rights" option within a Legacy software delivery policy was set to "Specified user" the password was encrypted incorrectly, and this caused the execution of the program to fail .	N/A
Unable to change the default time that a Managed Software Delivery policy ran before it terminated	With a Managed Software Delivery policy, it was not possible to change the default maximum execution time of 30 minutes. You set the execution time in the Advanced options dialog box on the Results-based actions tab in the Terminate after option.	N/A
Invalid cast in SMFAgent caused crash when OLE Automation string caching was disabled	If you were tracking down the memory leak and disabled the OLE Automation string cache by setting the system variable OANOCACHE=1 and then restarted the computer, your computer crashed.	N/A
Issues with importing very large packages into the Software Catalog	When you tried to import a very large package into the Software Catalog, the import could or take a very long time.	N/A
A deferred Managed Software Delivery installation failed if the deferral expired while the user was logged off	If you created a Managed Software Delivery policy that let the user defer the installation and the user deferred the installation, logged off, and logged on after the deferral expired, the defer dialog was not shown to the user when they logged back in and the installation did not run.	N/A

Table 1-14 Fixed Issues for Software Management Framework *(continued)*

Issue	Description	Article Link
Multiple detection and applicability rules could have the same name	In the Software Catalog, you can create multiple detection and applicability rules with the same name, which created confusion. A check is now performed to prevent the creation of rules with the same name.	N/A
An Installed Software Filter created from a software resource included the resource's dependencies	If a software resource had dependencies and you created an Installed Software Filter from the right-click menu of the software resource, the filter included the dependencies.	N/A
A Managed Software Delivery policy did not resume after a reboot task	If a Managed Software Delivery policy included a server reboot task, the job item that followed the reboot task tried to execute immediately instead of waiting until after the reboot.	N/A
Users could select software resources form the Quick Delivery Task dialog box that they did not have permission to view	In the Quick Delivery Task dialog box, the software resources that were listed in the software resource drop-down were not scoped. Consequently, a user can select software resources when they did not have permission to view those resources.	N/A
Unable to modify a software package using a French console	If you tried to edit a software package on a French console everything was grayed out and you could not change the settings.	N/A
A software resource was not updated when key values were changed	In the Software Catalog, when the name, version, or company of a software resource was changed, the resource key of the software resource was not updated with these new key values.	N/A
Changes to software package did not get downloaded by the Software Management Framework agent	With a Managed Software Delivery, when the contents of a software package changed, the Software Management Framework agent did not download the new files before a subsequent execution of the policy.	N/A
Export of a software package can sometimes fail	When a software package is exported, any files that were within the root directory of the package were being created as software installation files, which is not correct and in some cases caused the export to throw an exception.	N/A
Unable to add File Inventory when using fr-FR as IE Language	If you used fr-FR as the IE language and you edited a software resource on the File Inventory tab in the Software Catalog, an error occurred when you tried to add a file.	N/A

Table 1-14 Fixed Issues for Software Management Framework *(continued)*

Issue	Description	Article Link
Under certain conditions, Software Discovery was not able to complete	When different threads accessed the software cache at the same time, the SoftwareCache.xml was reset to a size of 0 which caused Software Discovery not to be able to complete.	N/A
Unable to delete a package from a Managed Software Delivery policy	If you created a software resource that had a package and assigned it to a Managed Software Delivery policy and then created a new package for the same software resource,disassociated the original package from the Managed Software Delivery policy and assigned the new package to the policy, the old package could not be deleted. It still appeared as associated to the policy. Even if you removed the software resource from the policy you could not delete the package.	N/A

Table 1-15 Fixed Issues for Data Connector

Issue	Description	Article Link
Now you can create an OLEDB or an ODBC Data Source in x64	Previously, you were not able to create an OLEDB or an ODBC Data Source in x64. An error message was displayed when you tried to create an OLEDB or an ODBC Data Source in x64. You have to download a component from http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=c06b8369-60dd-4b64-a44b-84b371ede16d for the data sources to work.	N/A
Cannot add columns to a Virtual Data Class	This is by design. You cannot add columns to a virtual data class because it is a representation of an external data source. If you want to add a column, then go to the datasource and either add a column to the base table or create a view.	N/A

Table 1-16 Fixed Issues for Network Discovery

Issue	Description	Article Link
ESX, ESX 3i,and Hyper V servers are not getting classified as virtual servers	This issue affected a limited set of customers and has been fixed.	TECH153669 N/A
VM created in the ESX server is now getting discovered	VM created in the ESX server was not getting discovered. This issue is fixed.	N/A

Table 1-16 Fixed Issues for Network Discovery *(continued)*

Issue	Description	Article Link
Discovery and Inventory now correctly handle the command sets that have multiple commands	Discovery and Inventory cannot correctly handle the command sets that had multiple commands. This issue is fixed and now the command-set option can be set for both Discovery and Inventory in the common Discovery engine.	N/A
Network Discovery now supports new VMware MIBs.	The VMware MIBs used previously did not find relevant information. This issue is fixed.	N/A
Dataclass 'Device Identification' now uses nvarchars	The dataclass 'Device Identification' used varchars instead of nvarchars. This created issues with the connector as the connector handles nvarchars for import. This issue is fixed.	N/A
Embedded ESX servers are now classified as Virtual Servers	Embedded VMware ESX servers were not classified as the Virtual servers and the virtual machines associated with the VMware ESX servers were not discovered. This issue is fixed.	N/A
Incorrect session attribute now does not cause hyper discovery to fail	Incorrect session attribute now caused hyper discovery to fail. This issue is fixed.	N/A

Table 1-17 Fixed Issues for Credential Manager, Connection Profiles, and the Pluggable Protocols Architecture

Issue	Description	Article Link
The discovery of devices was slow when VMware protocol was enabled	The discovery of devices was slow and not consistent when VMware protocol was enabled.	N/A
Memory leak in Altiris Event Receiver service does not happen now	You were unable to use event receiver for more than several hours. The Memory leaks resulted in the system not responding in about five hours.	N/A
The WSMAN plugin used to take long time for Enumerate Instances command	WSMAN plugin took 25 to 30 seconds for enumerating instances of certain classes.	N/A
Certain characters that are valid as AMT password characters were not accepted in the Altiris AMT credential dialog	The Notification Server error appeared for password containing some special characters. This issue is fixed.	N/A

Table 1-17 Fixed Issues for Credential Manager, Connection Profiles, and the Pluggable Protocols Architecture *(continued)*

Issue	Description	Article Link
PPA used to install some files into default location when Symantec platform is installed into custom path	If you installed Symantec platform into custom installation path such as drive letter:\somecustomfolder\altiris still certain files were found in the default C:\Program Files\Altiris\Altiris Agent\Agents\Pluggable Protocols Agent folder. Ideally, all the files and folders should install into custom installation path.	N/A
Now you can specify valid certificate file to WS-MAN protocol in Connection Profile settings	By default, Windows generates a certificate with .cer extension, while Connection Profile dialog did not accept such extensions. This issue is fixed.	N/A
Memory Leaks were observed in Windows 2008 after discovering 500 devices	After discovering 500 devices, memory leaks were observed in Windows 2008. After few days the CPU would stop responding.	N/A
EqualLogic inventory task runs successfully but inventory was not displayed	EqualLogic device inventory was not displayed in the Hardware summary page. The inventory task runs successfully but tables were not displayed in the Hardware Summary page. Now,the Hardware Summary page of an EqualLogic device displays the inventory of the device.	N/A
The Hardware Summary page for the VM status of the Hyper V server displayed incorrect status	Even if the VM was turned off , the Operational Status of the VM was shown as turned on . The Enabled State appeared blank. The column Operational Status is renamed as VM Power State. The column Enabled State is removed. A column Guest OS State is added. However, this info is only obtained through the SNMP and VMware protocols. When WS-MAN or WMI is used, this column is always et to unknown.	N/A

Table 1-18 Fixed Issues for UNIX/Linux/Mac

Issue	Description	Article Link
Remediation that is scheduled to run **At user login** did not work on Mac computers	With a Managed Software Delivery policy that targeted Mac computers, if you scheduled remediation to occur **At user login**, the remediation did not occur at that time.	N/A

Table 1-18 Fixed Issues for UNIX/Linux/Mac *(continued)*

Issue	Description	Article Link
Remediation and compliance checks sometimes did now run when configured to run when the computer started	With a Managed Software Delivery policy, if a compliance check or a remediation check was configured to run **At computer startup** on a UNIX/Linux/Mac client computer, the check sometimes did not run.	N/A
Option to run a Managed Software Delivery policy when a UNIX/Linux/Mac computer started did now work	When a Managed Software Delivery policy was scheduled to run **At computer startup**, it ran immediately when it arrived on a UNIX/Linux/Mac client computer.	N/A
Detection check did not work properly for rpm packages on a Linux client	With a Managed Software Delivery policy, if you installed an rpm package on a Linux client and the package was manually removed, the detection check sometimes failed to discover that the package was removed. When the detection checked failed, the package was not reinstalled.	N/A
Unable to install software on a UNIX computer after it was uninstalled	If you used a Managed Software Delivery policy to install and then uninstall software on a UNIX computer (Solaris, AIX, HP-UX), you could then not reinstall the software with the policy.	N/A
Command lines were created incorrectly for a package that was imported from subfolder	When you imported an rpm or Sun software package from a subfolder, the command line for the package was generated incorrectly.	N/A
Mac address of Mac OS X 10.6.5 clients was not sent	The Inv_AeX_AC_TCPIP table did not contain the Mac address for Mac OS X 10.6.5 clients because the address was not sent.	N/A
Software that was installed on a Mac client was not always detected	Some Mac software that was installed to the **Application** folder was not detected during a Software Discovery scan or by the detection rule of a Managed Software Delivery policy. Because the software was not detected, it was sometimes reinstalled although it was already installed and functional.	N/A
SSH keys were not migrated with an upgrade	If you upgraded from Notification Server 6.x or Symantec Management Platform 7.0, SSH keys for connecting to client computers were not migrated. The SSH keys are now migrated with the migration wizard.	N/A

Table 1-18 Fixed Issues for UNIX/Linux/Mac *(continued)*

Issue	Description	Article Link
The Symantec Management Agent Push Install page now lets you load computers reliably	Previously, in some cases when you attempted to add computers to the grid, a message "Data Could Not Be Loaded" appeared.	N/A
"Unspecified Dataloader Exception encountered for event data class AeX SWD Package" error message is logged to NS log during plug-ins rollout	If this error occurs, incorrect or incomplete information about agents or packages may be stored. This is a known issue for this release. N/A	N/A
The Symantec Management Console did not provide a way to purge old Audit Inventory information from the database	The Symantec Management Console did not provide a way to purge old Audit Inventory information from the database	TECH41981
The Purging Maintenance page did not let you purge data from Notification Server 7.0 reports	The Purging Maintenance page only allowed the purging of legacy Notification Server 6.x saved reports. It did not provide the ability to purge Notification Server 7.0 data snapshots.	TECH41488
When the ULM Agent was upgraded from Unix Agent 6.2 to ULM Agent 7.0 SP4 on AIX systems, the $PATH variable had no defined value (paths) in the agent's environment	If no absolute path was allocated, the execution of commands under the agent's environment would fail.	N/A

Other things to know

The other things to know about this release are separated into the following components:

- Symantec Installation Manager
  Table 1-19
- Notification Server
  Table 1-20
- Task Server
  Table 1-21

- Software Management Framework
  Table 1-22
- Network Discovery
  Table 1-23
- UNIX/Linux/Mac
  Table 1-24

Table 1-19 Things to know about Symantec Installation Manager

Issue	Description	Article Link
Two migration package files include the word "silent" in their name	The migration wizard installation package is installed at Program Files\Altiris\Symantec Installation Manger\MigrationPackage. The MigrationPackage folder contains four files. Two of these files include the word "silent" in their name. Use the migration package files that do not contain the word "silent" to install the migration wizard.	N/A
Command for setting up the required IIS settings	To set up the IIS required settings on the server before you install the Symantec Management Platform products, you can run the following command from the command prompt: `ServerManagerCmd.exe -install Web-WebServer AS-Web-Support Web-Mgmt-Compat Web-Asp NET-HTTP-Activation NET-Non-HTTP-Activ`	N/A
User requirements for migrating Notification Server data to Symantec Management Platform 7.1	If the logged on user is not a member of the Local Administrator group, the data migration wizard does not work.	TECH41187
Installation requirements for installing Symantec Installation Manager	You cannot install Symantec Installation Manager if the computer does not have a Temp folder.	TECH41182
Modify option on the Installed Products page is disabled	The ability to modify an installation is not supported in the current release of Symantec Installation Manager.	TECH41306
Number of applied licenses cannot be reduced	You cannot reduce the number of licenses that are applied to a product.	TECH41584
Symantec Installation Manager rejects some 6.x licenses	Symantec Installation Manager does not support license files that contain multiple certificates.	TECH41323

Table 1-19 Things to know about Symantec Installation Manager *(continued)*

Issue	Description	Article Link
Maximum computer name length for the Notification Server	The maximum length of the name for the Notification Server computer is 64 characters.	N/A
Inaccurate "In use" count on the Product Licensing page	On the Product Licensing page, the "In use" count can display a number that is smaller than the actual number of licenses that are in use for a product if the client computers are in sleep mode or turned off.	N/A
Problems with SQL Server cause the configuration of a product to fail	If there are problems with SQL Server during installation, Symantec Installation Manager installs the product but the configuration of the product fails.	N/A
Relaunching Symantec Installation Manager after canceling the migration wizard opens the Optional Installs page	With an on-box upgrade, if you don't select any of the items on the Optional Installs page and you cancel the installation when the migration wizard starts, Symantec Installation Manager opens to the Optional Installs page the next time it starts. To determine what products are being installed, click Back to access the Install New Products page or click Next to access the End User License Agreement page.	N/A
Workflow Solution is installed with Symantec Management Platform	Workflow Solution does not have its own install. When you install Symantec Management Platform, Workflow Solution gets installed.	N/A
Workflow servers are not uninstalled when you uninstall Symantec Management Platform	When you uninstall Symantec Management Platform, Workflow servers are not uninstalled. You have to manually uninstall Workflow servers.	N/A

Table 1-20 Things to know about Notification Server

Issue	Description	Article Link
You must configure web controls to support ActiveX	Typical error: Pop-up dialog box is blank when selecting Edit/New icon on "Update summary data" dialog. This is just one example of errors that can occur if Internet Explorer settings prevent the ActiveX control from running. For Notification Server to run properly, you must be able to install (or be prompted to install) ActiveX objects. Otherwise, you may see errors with jobs and task, among other functions. (This is by design.)	N/A

Table 1-20 Things to know about Notification Server *(continued)*

Issue	Description	Article Link
Take care when using the Query Builder in Basic mode	When you modify a report query using the Query Builder in Basic mode, be careful when you change the first condition of a Filter expression. When you change the first condition, the operator drop-down list reloads its contents. You might need to re-select the correct operator to successfully resolve the report query. Note that such unresolvable filter expressions are shown as “Blue” in the Query Builder.	N/A
You cannot export a policy to a local folder with full permissions on a Windows 2008r2 x64 server computer if you are using a console opened on localhost and if IE ESC (Enhanced Security Configuration) is turned on for Administrators	When you attempt to save such a policy to a local folder with full permissions, the following message is displayed: "You don’t have permission to save in this location... Would you like to save in the My Documents folder instead?" This issue occurs only when Internet Explorer ESC (Enhanced Security Configuration) is turned on for Administrators. To work around this issue, turn off Internet Explorer ESC.	N/A
The Manage Computers list sometimes shows duplicate entries of the same computer after SOI task	This is the expected behavior if the name of a computer changes at the same time as its MAC address or BIOS unique identifier. In this scenario it cannot be identified as the same computer. This issue is much more common for virtual machines because by default they use randomly generated MAC addresses, which can change. The workaround for this issue is to ensure that all VM computers have statically-defined MAC addresses before you change the computer name/domain.	N/A
Windows 2000 clients are not upgraded when you upgrade to SMP 7.1	Windows 2000 clients that have the 6.x Altiris Agent are not upgraded. This is by design: Windows 2000 is not supported in Symantec Management Platform 7.1	N/A
You cannot add domain groups to Symantec Management Platform Security roles	If you attempt to add a domain user to a security role (menu path: Settings > Security > Roles, on the Membership tab) an error message is displayed on the Add User dialog box. This is because adding domain groups directly into a security role is no longer a supported scenario. Symantec Management Platform 7.1 only supports adding an SMP role or an SMP account into a role.	Tech144089

Table 1-20 Things to know about Notification Server *(continued)*

Issue	Description	Article Link
Database upgrades cannot be performed across different collations	Symantec Management Platform does not support upgrading across different collations. If you attempt to do this, the database reconfiguration fails with an error message saying "Cannot resolve the collation conflict". The database and database server collations must match.	N/A
Symantec Management Agent icon may not be removed when the Symantec Management Agent is uninstalled	When you uninstall the Symantec Management Agent from a Windows 7 computer, the Symantec Management Agent icon is not removed. The Symantec Management Agent icon remains listed in the Customize Icons list. To view the Customize Icons list on a Windows 7 computer, do one of the following: ■ Right-click the taskbar and then select Properties > Customize. ■ Click the Show hidden icons option on the toolbar.	TECH44030
Symantec Management Agent icon may not appear in the system tray	When you install the Symantec Management Agent, you can choose to display the Symantec Management Agent icon in the system tray on the client computer. However, on Windows 7 computers, the Symantec Management Agent icon does not appear in the system tray.	TECH44034
Attempting to add Data Classes to a new Resource Type sometimes fails with a script error	If you create a new resource type (left pane: Settings > Notification Server > Resource and Data Class Settings > Resource Types > Asset Types, then right-click and select New > Resource Type) and then in the Resource Type Edit page, click the Add Data Classes option, a script error message is displayed. Note that you must have CMDB Solution installed to access the New Resource Type page. This issue is related to your Internet Explorer browser configuration which is preventing the necessary ActiveX control from loading. To enable the data class picker (the AexTreeCtrl ActiveX control) to load successfully, you need to enable Automatic prompting for ActiveX controls under the Internet Explorer security settings.	TECH46224
Package Replication Solution will not work on Notification Server 7.1	Package Replication Solution will not work on Notification Server 7.1 because the package replication rules created using this solution on Notification Server 6.0 SP3 cannot be upgraded to the Replication Rules equivalent that exists in Notification Server 7.1. Errors appear when you attempt to use the package replication importer found in the migration wizard.	TECH41330

Table 1-20 Things to know about Notification Server *(continued)*

Issue	Description	Article Link
If the Symantec Management Agent is using a proxy server, the client task agent may fail to register	When the Symantec Management Agent is using a proxy server, it fails to post events to Notification Server correctly. This results in the client task agent not being registered. Note that communication involving configuration updates, basic inventory, downloading package snapshots, and downloading packages is not affected.	TECH41484
The user name for the Symantec Management Agent Connectivity Credential cannot include any special characters	The user name for the Symantec Management Agent Connectivity Credential cannot include any special characters	TECH41492
In some circumstances the Symantec Management Console displays the Resource Manager portal page	If you open the Resource Manager while the Symantec Management Console is open, and then refresh the Console page, the Console displays the Resource Manager portal page. To restore the original page in the Symantec Management Console, you need to select the appropriate menu option.	TECH41499
NSSetup.aspx is no longer a supported method for reconfiguring the database from a corrupted console	Symantec Installation Manager (SIM) does not handle this scenario either. You need to use the aexconfig /configureall command.	HOWTO9821
Track role deletion is now on by default	With Symantec Management Platform 7.0 SP5, "SyncRoleMembershipExactlyDuringReplication" and "TrackRoleDeletionForHierarchy" were added to CoreSetting.config. With Symantec Management Platform 7.1, "TrackRoleDeletionForHierarchy" was removed from ConeSetting.config. The functionality of "TrackRoleDeletionForHierarchy" is now on by default. If you want to turn off track role deletion , contact technical support.	N/A
Unable to roll out the Symantec Management Agent when SSL is used to access the platform	During installation of the Symantec Management Platform products, a **Use SSL for accessing management platform** option appears on the **Notification Server Configuration** page. If you select this option, then you must install a self-signed certificate on your client computers before you deploy the Symantec Management Agent to these computers. You can use an Active Directory group policy to install the certificate before the agent roll out.	N/A

Table 1-21 Things to know about Task Server

Issue	Description	Article Link
Pop-up dialog box is blank when selecting Edit/New icon on "Update summary data" dialog	For Notification Server to run properly, you must be able to install (or be prompted to install) ActiveX objects. If your IE settings prevent the ActiveX control from running, you will see errors when working with jobs and tasks. This is by design.	N/A
Inconsistent replication of tasks in a hierarchy	The replication of tasks and task instances within a hierarchy has inconsistent behavior with tasks and instances sometimes being replicated immediately when the task is run, but other times waiting for the hierarchy schedules to be run.	N/A
System.Net.Sockets.SocketException observed while trying to restart the Task server services (Altiris Object Host service)	In some cases the agent cannot register with task server, preventing users from running tasks on agent computers. For more information see http://support.microsoft.com/kb/960718.	N/A
A window is not displayed when cmd.exe is running in Task Manager as System even though the Show Script in a Normal Window option is selected	A new Windows 2008 security feature called "Session isolation" most likely causes this error.	N/A

Table 1-22 Things to know about Software Management Framework

Issue	Description	Article Link
Terminology	A list of terminology used in Software Management Framework.	DOC1717
Software Discovery policy enabled by default	By default, the Software Discovery policy is scheduled to run two times per week on all the computers that contain the Software Management Framework agent.	N/A
Java runtime required for importing packages into the Software Management Framework	If you do not have JRE 1.6 or higher installed, you get an error message when you try to import or add a package into the Software Management Framework.	HOWTO9940

Table 1-22 Things to know about Software Management Framework *(continued)*

Issue	Description	Article Link
Accessing the Symantec Management Console remotely can cause some Software Catalog functionality not to work	If you access the Symantec Management Console remotely from a computer that is not part of the Notification Server admin domain, some of the functionality in the Software Catalog does not work.	TECH127274
Replicating a single resource does not replicate dependent resources	When you replicate a single resource, any dependent resources are not automatically replicated. If you want dependent resources to be replicated, you must replicate them as well. For example, if you replicate a Managed Software Delivery policy that has a detection rule, you must also replicate the detection rule or the policy will fail.	TECH46168
Powering on a computer with a Managed Software Delivery	When you schedule a Managed Software Delivery, the Power on if necessary option only powers on a client computer when the policy is initially enabled and saved. It does not wake up a client computer after the policy is on the client computer.	N/A
When a data provider task is identified by its description	If you create a new schedule for a data provider task that includes a description and you schedule the task to run in the future, the task is not identified by the description until the task runs.	N/A
A Quick Delivery task does not execute in hidden mode for an EXE	If you deliver an EXE with a Quick Delivery task and you select Hidden in the Display window drop-down list on the Run Options tab of the Advanced options, the task may not get executed in the hidden mode. Whether the installation is hidden depends on whether the EXE obeys the request to hide the installation.	N/A
Symbolic links are lost if TAR/TAR.GZ/TAR/Z packages are unzipped or repackaged on a Windows computer	To preserve symbolic links, do not unzip or repackage these packages on a non-UNIX computer.	N/A

Table 1-23 Things to know about Network Discovery

Issue	Description	Article Link
Using Connection Profiles Network Discovery tasks use	Connection Profiles to configure the protocols that are used to communicate with network devices.	HOWTO9348

Table 1-23 Things to know about Network Discovery *(continued)*

Issue	Description	Article Link
Importing .MIB files on Symantec Management Platform 7.0		HOWTO9709
Symantec Management Platform Security Privileges		DOC1740
Scheduling a Network Discovery task	If you schedule a Network Discovery task to run on a recurring basis, you won't be able to stop that task unless you either delete the task or cancel the schedule by deleting the next scheduled occurrence of it in Manage > Jobs and Tasks.	N/A

Table 1-24 Things to know about UNIX/Linux/Mac

Issue	Description	Article Link
ULM agent cannot be installed onto HP-UX if CSH is set as root shell	When you push-install the ULM agent onto HP-UX computers that have CSH set as boot-shell for root, links to the agent's binaries location (commands) are created. However, on some systems such as HP-UX ia64 11.23-11.31, these binaries/commands cannot be executed in user sessions. The absolute path needs to be specified.	TECH133272
Legacy 6.x SWD tasks sometimes ignore scheduling and execute as soon as they arrive on ULM 7.1 client systems	In some cases the 'Run once ASAP' option is checked in the legacy SWD task. This option supersedes any scheduled time or maintenance window. This is by design. If this option is not deselected, the software delivery task will be executed as soon as a policy arrives on the client systems, overriding any schedule. When you are adding schedules to a Legacy Software Delivery task, you should uncheck the 'Run Once ASAP' option unless you intend the task to execute at the first opportunity.	N/A
Push-installing the Symantec Management Agent for UNIX, Linux, and Mac to a computer that has the secondary shell configured in .profile may fail with timeout errors	If you attempt to push install the Symantec Management Agent for UNIX, Linux, and Mac to a computer system that has a secondary shell configured in .profile, the push install may fail due to a timeout error. The secondary shell is any shell other than the configured shell in /etc/passwd for user root in /etc/profile, .profile, or .bash_profile.	TECH44831

Table 1-24 Things to know about UNIX/Linux/Mac *(continued)*

Issue	Description	Article Link
Installing the Symantec Management Agent for UNIX, Linux, and Mac on an HP-UX 11.00 computer produces a “Memory fault (coredump)” error	This is due to a defect in the dynamic linker on the HP-UX 11.00 computer. You need to apply the appropriate patch.	TECH42006
Daemons running on Mac 10.6 in root bootstrap context cannot execute commands using the nohup utility	This is a system limitation caused by Mac OS 10.6 OS design and can’t be overridden. This limitation may affect commands that are executed by SWD/SMF tasks, or Script tasks.	TECH47689
Managed and quick software deliveries may fail on some HP-UX systems	Managed and quick software deliveries that contain a tar.bz2 or .bz2 related command line may fail on some HP-UX systems.	TECH137859
Trailing slash is required for an alternate download location for a Linux package server	A package server configuration has an Alternate Download Location option. With a Linux package server, you can set this option with a Windows-style path. It is then converted to UNIX-style so that C:\path\ becomes /path/. However, for proper conversion, a trailing slash is required. If the trailing slash is missign as in "C:\path", the path is not converted correctly.	N/A

Documentation that is installed

Table 1-25 The product installation includes the following documentation:

Document	Description	Location
Help	Information about how to use this product. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The **Documentation Library**, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ The F1 key when the page is active. ■ The **Context** command, which is available in the Symantec Management Console on the **Help** menu.
Symantec Management Platform Help	Information about how to use the Symantec Management Platform	The **Documentation Library**, which is available in the Symantec Management Console on the **Help** menu.
Symantec Management Platform User Guide	The user guide in PDF format	The **Documentation Library**, which is available in the Symantec Management Console on the **Help** menu or the Symantec Management Platform Documentation page. **Note:** For details about configuring security, please refer to "Setting up Symantec Management Platform security" in the Symantec Management Platform User Guide. This PDF contains updated information to help guide you through security setup and configuration.

Other information

Table 1-26 For more information, you can use the following resources:

Document	Description	Location
Altiris IT Management Suite 7.1 from Symantec Planning and Implementation Guide	Information about capacity recommendations, design models, scenarios, test results, and optimization best practices to consider when planning or customizing ITMS.	IT Management Suite Planning and Implementation Guide
Symantec Management Platform User Guide	Information about using the Symantec Management Platform.	Symantec Management Platform Documentation page When setting up security, see "Setting up Symantec Management Platform security" in the Symantec Management Platform User Guide. This PDF contains updated information to help guide you through security setup and configuration.
Symantec Management Platform Release Notes	Information about new features and important issues in the Symantec Management Platform.	Symantec Management Platform Documentation page
Symantec Management Platform Installation Guide	Information about using Symantec Installation Manager to install the Symantec Management Platform products.	http://go.symantec.com/sim_doc
Knowledge base	Articles, incidents, and issues about this product.	SymWISE support page
Symantec Connect (formerly the Altiris Juice)	An online magazine that contains best practices, tips, tricks, and articles for users of this product.	Symantec Connect page